УДК 004.4

А.В. Зазимко
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення статистичного аналізу та фільтрації даних зі змінних носіїв

В останні роки в Україні намітився перехід від традиційної форми подання документів до їхнього електронного подання. Перехід до електронного документообігу з використанням змінних носіїв несе цілий ряд переваг, серед яких: істотне скорочення строків розробки й проходження документів у структурі підприємства, спрощення формування й пересилання пакетів документів між підприємствами, що, у свою чергу, припускає відчутну економічну вигоду. Не дуже давно були прийняті державний стандарт електронного цифрового підпису (ЕЦП) ДСТУ 4145-2002 і Закон «Про електронний цифровий підпис», що є вірним свідченням серйозних кроків у даному напрямку. Із прийняттям закону «Про електронний документ» електронні документи знайдуть свою юридичну чинність і зможуть замінити традиційні документи.

Крім правової бази, серйозним стримуючим фактором на шляху переходу до електронних документів (ЕД) є нерозв'язаність ряду серйозних питань, пов'язаних із забезпеченням збереження конфіденційності інформації в системах електронного документообігу з використанням змінних носіїв. Зокрема, перехід до ЕД припускає їхню передачу в електронному виді по різних каналах зв'язку, у тому числі з використанням змінних носіїв. З огляду на сучасний стан, а також перспективи розвитку систем зв'язку й телекомунікації, очевидним є широке використання для цих цілей відкритих каналів зв'язку й глобальних мереж. Збереження конфіденційності інформації при її передачі по відкритих каналах зв'язку може бути забезпечене методами як криптографічного, так і стеганографічного методу збереження конфіденційності інформації. При цьому варто помітити, що жоден із зазначених напрямків на поточному рівні розвитку не в змозі самостійно вирішити всі завдання, пов'язані із збереження конфіденційності інформації в електронному документообігу. Крім того, рішення ряду специфічних завдань можливо тільки при спільному погодженому застосуванні методів криптографії й стеганографії.

Таким чином, актуальною проблемою є забезпечення збереження конфіденційності інформації в системах електронного документообігу з використанням змінних носіїв шляхом погодженого застосування методів криптографії й стеганографії.

Теоретичний аспект сформульованої проблеми складається у визначенні й обґрунтуванні можливих шляхів забезпечення збереження конфіденційності інформації при передачі електронних документів з використанням змінних носіїв та відкритих каналів зв'язку; пошуку механізмів забезпечення скритності найбільш значимої для підприємства частини документообігу від потенційних конкурентів; визначенні шляхів і способів протидії небезпечним для ІБ підприємства діям інсайдерів.

Практичний аспект проблеми полягає: у розробці механізмів забезпечення скритності електронного документообігу з використанням змінних носіїв від засобів конкурентної розвідки; розробці методів, алгоритмів і моделей програмних засобів, що дозволяють забезпечити безпеку електронних документів при їхній передачі з використанням змінних носіїв та по відкритих каналах зв'язку; розробці методів,

алгоритмів і моделей програмних засобів схованого маркування електронних документів при інформаційному обміні.

Об'єктом дослідження є процес виявлення несанкціонованого витоку конфіденційної інформації. Предметом дослідження – статистичний аналіз та фільтрація даних зі змінних носіїв.

Ціль роботи – підвищення ефективності методу збереження конфіденційності інформації в багатокористувальницьких розподілених системах електронного документообігу з використанням змінних носіїв на базі сучасних технологій схованого зв'язку.

Завдання дослідження: 1) Аналіз уразливостей і розробка класифікації стеганографічних атак на системи схованої передачі електронних документів з використанням змінних носіїв. 2) Оцінка ефективності сучасних стеганографічних методів і визначення границь їхньої застосовності, розробка методу й визначення критеріїв оцінки практичної стійкості стеганографічних методів методу збереження конфіденційності інформації. 3) Дослідження можливості побудови теоретично стійких стеганографічних методів і систем. 4) Розробка моделей, принципів і проектних рішень на базі методів криптографії й стеганографії для створення перспективних засобів збереження конфіденційності змісту електронних документів, що володіють високою теоретичною й практичною стійкістю, обґрунтування ефективності запропонованих рішень. 5) Розробка нових стеганографічних методів, орієнтованих на використання в розроблювальних системах методу збереження конфіденційності інформації, які б відповідали необхідним вимогами й мали високий рівень стійкості. 6) Розробка методів, алгоритмів, моделі й архітектури системи схованого маркування й перевірки маркування електронних документів у системах електронного документообігу з використанням змінних носіїв й базах даних.

Для рішення завдань використані методи теорії інформації й зв'язку, теорії ймовірностей і математичної статистики, методи обчислювальної математики, теорії ухвалення рішення, теорії інформаційної безпеки й розподілених систем.

Список літератури

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теор. и практ..–К.:«МК-Пресс», 2006.–288 с.
2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.
3. Хорошко В.А., Шелест М.Е. Введение в компьютерную стеганографію. – К., 2002. – 140 с.
4. Корольов В.Ю. Планування досліджень методів стеганографії та стегоаналізу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко, М.Л. Горінштейн // Вісник Хмельницького нац. ун-ту №4, 2011. – 187-196 с.
5. Корольов В. Ю. RS-стеганоаналіз. Принципи роботи, недоліки та концепція метода його обходу / В. Ю. Корольов, В. В. Поліновський, В. А. Герасименко // Вісник Вінницького політехн. Ін-ту.–2010.–№6.–С.66-71.
6. Кущ А.В. Использование алгоритмов стеганографії при проведении компьютерно-технической экспертизы / А.В. Кущ // VI Всеросс. межвуз, конф. молодых ученых – СПб: СПбГУ ИТМО, 2009.

УДК 004.056:621.3(043.3)

Н.В. Захарчук
Науковий керівник – Пепа Ю.В., канд. техн. наук, доцент
Національний авіаційний університет

Ідентифікація радіовипромінювань

Вступ. На сьогоднішній день невід'ємною частиною будь-якого підприємства чи банку є масове використання електронної апаратури, тому виникає проблема захисту інформації від зовнішнього впливу, адже будь-який пристрій при роботі створює електромагнітне поле випромінювання. В результаті створюються канали технічного витоку інформації [1], одним із самих небезпечних є радіоканал витоку